CLAIMS

What is claimed is:

1. A method for a receiver to verify a security certificate for a sender comprising the steps of:

receiving a first security certificate associated with the sender and storing the first security certificate in a location accessible to the receiver;

updating the first security certificate in the location accessible to the receiver if the first security certificate is changed or revoked;

receiving a second security certificate from the sender when identity of the sender needs to be verified;

comparing the second security certificate to the first security certificate; and

confirming the sender's identity only if the second security certificate matches the first security certificate for the sender.

2. The method of Claim 1, wherein the step of updating the first security certificate comprises:

removing the first certificate from the location accessible to the receiver if the first certificate is revoked; and

replacing the first certificate in the location accessible to the receiver if the first certificate is changed.

3. The method of Claim 2, wherein the removing step is performed if the first certificate is known to have been revoked for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate.

4. The method of Claim 2, wherein the replacing step is performed if the first certificate is known to have been changed for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate.

5. The method of Claim 1, wherein the storing step comprises storing the first security certificate in a directory service.

6. The method of Claim 5, wherein the directory service is a Lightweight Directory Access Protocol directory.

7. The method of Claim 1, wherein the first certificate is known to have been granted by a certificate authority.

8. The method of Claim 1, wherein the first certificate is known to have been obtained in a trusted domain.

9. The method of Claim 1, wherein the step of comparing the first certificate and second certificate comprises comparing a computer memory representation of each certificate.

10. The method of Claim 1, wherein the sender is a client and the receiver is a server.

11. The method of Claim 10, wherein the receiver is an authentication, authorization, and accounting server.

12. The method of Claim 1, wherein the sender is a server and the receiver is a client.

13. The method of Claim 1, wherein the communication between the sender and receiver is in a protocol that requires the inclusion of a digital certificate.

14. The method of Claim 13, wherein the protocol is selected from the group consisting of the Extensible Authentication Protocol and Transport Level Security protocol, the Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security protocol.

15. The method of Claim 1, wherein the second certificate is known to have been signed by a certificate authority.

16. The method of Claim 15, further comprising the step of decrypting the second certificate using a public key associated with the certificate authority, whereby the receiver verifies that the certificate authority has signed the second certificate.

17. The method of Claim 1, further comprising the step of validating that the sender has a private key corresponding to a public key in the second certificate, this step comprising the steps of:

receiving a message encrypted with the sender's private key; and

decrypting the message using the sender's public key.

18. A method for a server to verify a security certificate for a client comprising the steps of:

copying a first security certificate associated with the client to a location accessible to the server;

updating the first security certificate in the location accessible to the server if the first certificate is changed or revoked;

receiving a second security certificate from the client when identity of the client needs to be verified;

comparing the second security certificate to the first security certificate; and

confirming the client's identity only if the second security certificate matches the first security certificate.

19. The method of Claim 18, wherein the step of updating the first certificate comprises:

removing the first certificate from the location accessible to the server if the first certificate is revoked; and

replacing the first certificate in the location accessible to the server if the first certificate is changed.

20. The method of Claim 19, wherein the removing step is performed if first certificate is known to have been revoked for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate.

21. The method of Claim 19, wherein the replacing step is performed if first certificate is known to have been changed for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate.

22. The method of Claim 18, wherein the location accessible to the server is a Lightweight Directory Access Protocol directory.

23. The method of Claim 18, wherein the first certificate is known to have been granted by a certificate authority.

24. The method of Claim 18, wherein the first certificate is known to have been obtained in a trusted domain.

25. The method of Claim 18, wherein the server is an authentication, authorization, and accounting server.

26. The method of Claim 18, wherein the step of comparing the first certificate and second certificate comprises comparing a computer memory representation of each certificate.

27. The method of Claim 18, wherein the communication between the client and server is in a protocol that requires the inclusion of a digital certificate.

28. The method of Claim 27, wherein the protocol is selected from the group consisting of the Extensible Authentication Protocol and Transport Level Security protocol, the Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security protocol.

29. The method of Claim 18, wherein the second certificate is known to have been signed by a certificate authority.

30. The method of Claim 29, further comprising the step of decrypting the second certificate using a public key associated with the certificate authority, whereby the server verifies that the certificate authority has signed the second certificate.

31. The method of Claim 18, further comprising the step of validating that the client has a private key corresponding to a public key in the second security certificate, this step comprising the steps of:

receiving a message encrypted with the client's private key; and

decrypting the message using the client's public key.

32. A method for a client to verify a security certificate for a server comprising the steps of:

receiving a first security certificate associated with the server and storing the first security certificate in a location accessible to the client;

updating the first security certificate in the location accessible to the client if the first security certificate is changed or revoked;

receiving a second security certificate from the server when identity of the server needs to be verified;

comparing the second security certificate to the first security certificate; and

confirming the server's identity only if the second security certificate matches the first security certificate for the server.

33. The method of Claim 32, wherein the step of updating the first certificate comprises:

removing the first certificate from the location accessible to the client if the first certificate is revoked; and

replacing the first certificate in the location accessible to the client if the first certificate is changed.

34. The method of Claim 33, wherein the removing step is performed if the first certificate is known to have been revoked for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate.

35. The method of Claim 33, wherein the replacing step is performed if the first certificate is known to have been changed for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate.

36. The method of Claim 32, wherein the step of comparing the two certificates comprises comparing a computer memory representation of each certificate.

37. The method of Claim 32, wherein the server is an authentication, authorization, and accounting server.

38. The method of Claim 32, wherein the communication between the client and server is in a protocol that requires the inclusion of a digital certificate.

39. The method of Claim 38, wherein the protocol is selected from the group consisting of the Extensible Authentication Protocol and Transport Level Security protocol, the Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security protocol.

40. The method of Claim 32, wherein the second certificate is known to have been signed by a certificate authority.

41. The method of Claim 40, further comprising the step of decrypting the second certificate using a public key associated with the certificate authority, whereby the client verifies that the certificate authority has signed the second certificate.

42. The method of Claim 32, wherein the server is one of a plurality of load balanced servers and each server of the plurality of load balanced servers has an identical security certificate, whereby the client need not know to which of the plurality of servers it is attached.

43. The method of Claim 32, further comprising the step of validating that the sender has a private key corresponding to a public key in server's security certificate, this step comprising the steps of:

receiving a message encrypted with the server's private key; and

decrypting the message using the server's public key.

44. A computer-readable medium carrying one or more sequences of instructions which, when executed by one or more processors, causes the one or more processors to perform the steps of:

receiving a first security certificate associated with the sender and storing the security certificate in a location accessible to the receiver;

updating the first security certificate in the location accessible to the receiver if the first security certificate is changed or revoked;

receiving a second security certificate from the sender when identity of the sender needs to be verified;

comparing the second security certificate to the first security certificate; and

confirming the sender's identity only if the second security certificate matches the first security certificate for the sender.

45. A system comprising:

a local area network; and

two or more devices communicatively coupled to the local area network; wherein one or more of the devices are configured to perform the steps of:

receiving a first security certificate associated with the sender and storing the security certificate in a location accessible to the receiver;

updating the first security certificate in the location accessible to the receiver if the first security certificate is changed or revoked;

receiving a second security certificate from the sender when identity of the sender needs to be verified;

comparing the second security certificate to the first security certificate; and

confirming the sender's identity only if the second security certificate matches the first security certificate for the sender;

and one or more of the devices are configured to perform the steps of:

copying the first certificate to a location accessible to the sender;

updating the first certificate in the location accessible to the sender if the certificate is changed or revoked; and

sending the first certificate to a receiver when the identity of the sender needs to be verified.